KN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/978,026	10/17/2001	Martin Tasler	2000P15975US	3824

466 7590 01/20/2006

YOUNG & THOMPSON
745 SOUTH 23RD STREET
2ND FLOOR
ARLINGTON, VA 22202

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 01/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/978,026	TASLER, MARTIN	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 October 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 October 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Applicant's arguments/amendments with respect to amended claims 1-8 and newly presented claims 9-13 filed 10/14/2005 have been fully considered but they are not persuasive. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Previous drawing and claim objections have been withdrawn due to the amendment filed 10/14/2005.

Response to Arguments

Applicant contends that the prior arts of record fail to teach/suggest the feature where the central server stores "two different groups of features from which an individual-referenced feature is randomly selected." Examiner respectfully disagrees. Wizig teaches the essential elements of using a central server, where that central server contains various software databases in order to store information that can be used during a user's attempt to gain access (col. 7, lines 32-38). Specifically, Wizig discloses a registration database which contains user information that is used in order to authenticate the user (col. 7, lines 58-66). Wizig also teaches a member demographics database that includes other features, such as the user's login id, date of birth, and social security number. These two databases contain the elements of the second feature group. Ikebata et al. suggest motivation for why it would be beneficial to randomly select a feature in a system where access is to be controlled. Ikebata et al. suggest that if the user has no knowledge of the type of data that will be required during authentication it is harder for an imposter to impersonate a user in order to gain access to the system (paragraph 12).

Furthermore, Ikebata et al. teach a first feature group that contains various types of biometric data. As it is known, two-factor authentication is more secure than only using one form of authentication. Further, it is also known that biometrics is the strongest form for authentication. Knowing these factors, since Ikebata et al. teach using randomly selected biometric data (paragraph 12) and Wizig teaches that there are a plurality of software databases in the central server (col. 7, lines 32-38), it follows that the Wizig reference could be modified to also include the first feature group in the central server. One of ordinary skill in the art at the time the invention was made would have been motivated to modify the Wizig reference in that manner in order to make the system more secure and to diminish the number of intruders that could wrongfully access the system based on the knowledge that two-factor authentication is more secure that one-factor authentication.

Due to the reasons stated above, the Examiner maintains rejections with respect to amended claims 1-8 and newly presented claims 9-13. Wizig teaches the limitations that the Applicant suggests distinguish from the prior art. Furthermore, Ikebata et al. in combination with Wizig teach the limitations not explicitly disclosed by Wizig. Therefore, it is the Examiner's conclusion that amended claims 1-8 and newly presented claims 9-13 are not patentably distinct or non-obvious over the prior art of record as presented.

Claim Objections

Claim 13 is objected to because of the following informality: lines 8-9 contain two choices labeled with the letter "(e)." The second "(e) a genetic fingerprint" should be modified to appear as follows "(f) a genetic fingerprint."

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wizig, U.S. Patent No. 6,735,569, and further in view of Ikebata et al., EP Patent No. 0895750 A2.

As per claim 1:

Wizig substantially teaches the method for identifying a user, in which at least one person-specific feature of the user, is requested by a central server and is transmitted to the central server by an input appliance of a user computer device via a telecommunication link (col. 6, line 61 - col. 7, line 47 and fig. 1, element 200), in particular over the Internet (fig. 1, element 140), and is compared with stored user data (col. 10, lines 36 – col. 11, line 31), and he at least one person-specific feature being selected in a second feature group comprising the user name and/or the date of birth and/or a user number and/or a secret number (fig. 10).

Not explicitly disclosed by Wizig is the at least one person-specific feature being selected by the central server on the basis of the random principle from a plurality of features recorded in a first feature group comprising the print from at least one finger and/or the image of the iris of at least one eye and/or a voice sample and/or a sample signature and/or an image of at least part of the user and/or the genetic fingerprint.

However, Ikebata et al. teach that information regarding person-specific features can be maintained in storage, as a first feature group, in order to authenticate a user by using biometrics

such as fingerprints, voiceprint, and/or iris patterns. Furthermore, Ikebata et al. teach that the user's computer device has a camera as an inputting means. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wizig to use biometrics, as well as an inputting means to allow the user to respond to the request for biometric data, in order to have a stronger means of authentication. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ikebata et al. in paragraph 5.

Furthermore, Ikebata et al. teach that the person-specific feature can be randomly selected from the possible data that exists in the registered user's data record. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wizig to randomly select the means of authentication to further strengthen the authentication process. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ikebata et al. in paragraphs 42-47.

As per claim 2:

Wizig and Ikebata et al. substantially teach the method as claimed in claim 1. Furthermore, Ikebata et al. teach the method characterized in that a plurality of person-specific features are selected and requested on the basis of the random principle (paragraphs 42-47).

As per claim 4:

Wizig and Ikebata et al. substantially teach the method as claimed in claim 1. Furthermore, Wizig teaches the method characterized in that the data are transmitted in

encrypted form (col. 7, lines 16-20).

As per claim 5:

Wizig substantially teaches a system for identifying a user having at least one central server (col. 6, line 61 - col. 7, line 47 and fig. 1, element 200) having a database containing person-specific features for users (col. 7, line 58 – col. 8, line 7 and fig. 2, element 1000), having at least one external, user computer device which communicates with the server over the Internet (col. 6, lines 15-24 and fig. 1, element 110) and containing a second feature group comprising the user name and/or the date of birth and/or a user number and/or a secret number (fig. 10).

Not explicitly disclosed by Wizig et al. is the user computer device having at least one input appliance which can be used for the server to request at least one person-specific feature and for transmitting said feature to the server, the person-specific features of a user being stored on the server in a person-specific data record (3, 4) containing a first feature group comprising the print from at least one finger and/or the image of the iris of at least one eye and/or a voice sample and/or a sample signature and/or an image of at least part of the user and/or the genetic fingerprint and the at least one person-specific feature (5) requested being able to be selected on the basis of the random principle from the features in both feature groups (3a, 3b, 4a, 4b).

However, Ikebata et al. teach that information regarding person-specific features can be maintained in storage, as a first feature group, in order to authenticate a user by using biometrics such as fingerprints, voiceprint, and/or iris patterns. Furthermore, Ikebata et al. teach that the user's computer device has a camera as an inputting means. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wizig to use biometrics, as well as an inputting means to allow the user to respond to the

request for biometric data, in order to have a stronger means of authentication. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ikebata et al. in paragraph 5.

Furthermore, Ikebata et al. teach that the person-specific feature can be randomly selected from the possible data that exists in the registered user's data record. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wizig to randomly select the means of authentication to further strengthen the authentication process. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ikebata et al. in paragraphs 42-47.

As per claim 6:

Wizig and Ikebata et al. substantially teach the system as claimed in claim 5. Furthermore, Ikebata et al. teach the system characterized in that the input appliance of the user computer device (7, 13) comprises at least one camera (11) and/or at least one microphone and/or at least one means (17) for recording a fingerprint (par. 13).

As per claim 7:

Wizig and Ikebata et al. substantially teach the system as claimed in claim 5. Not explicitly disclosed is the system characterized in that a plurality of central servers having identical databases are provided. However, Wizig teaches that the central server can have a plurality of software servers. Furthermore, since the central server holds information regarding healthcare service providers, having a plurality of central servers with identical databases could

be used in order to accommodate to different geographical locations. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wizig to have a plurality of central servers having identical databases. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Wizig in col. 7, lines 32-46 and col. 26, lines 46-50.

As per claim 8:

Wizig and Ikebata et al. substantially teach the system as claimed in claim 5. Furthermore, Wizig teaches the system characterized in that the server (2) and/or the user computer device (7, 13) comprise a means for data encryption and decryption (col. 7, lines 16-20).

III. Claims 3 and 9-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wizig U.S. Patent No. 6,735,569 and Ikebata et al. EP Patent No. 0895750 A2, and further in view of Brookner, U.S. Patent No. 6,256,616.

As per claim 3:

Wizig and Ikebata et al. substantially teach the method as claimed in claim 2. Not explicitly disclosed is wherein the at least one of the person-specific features is selected and requested. However, Brookner teaches that a biometric feature can be the feature that is always selected in combination with the other data requested. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wizig to always choose at least one of the person-specific features based on the known principle that the use of biometrics for authentication is the strongest single-factor authentication and furthermore

combining biometrics with another factor of authentication forms two-factor authentication which is also known to be better than single-factor authentication. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Brookner in col. 7, lines 32-46 and col. 26, lines 46-50.

As per claim 9:

Wizig and Ikebata et al. substantially teach the method as claimed in claim 1. Not explicitly disclosed is wherein the first feature group includes a plurality of different ones of the person-specific features for the user and wherein at least one of the person-specific features in the first group always s selected and requested when identifying the user. However, Brookner teaches that a biometric feature can be the feature that is always selected in combination with the other data requested. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wizig to always choose at least one of the person-specific features based on the known principle that the use of biometrics for authentication is the strongest single-factor authentication and furthermore combining biometrics with another factor of authentication forms two-factor authentication which is also known to be better than single-factor authentication. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Brookner in col. 3, line 38 - col. 4, line 10.

As per claim 10:

Wizig, Ikebata et al., and Brookner substantially teach the method of claim 9. Furthermore, Brookner teaches wherein a plurality of the person-specific features are randomly selected and requested (col. 3, lines 55-57).

As per claim 11:

Wizig and Ikebata et al. substantially teach the method as claimed in claim 5. Not explicitly disclosed is wherein the first feature group includes a plurality of different ones of the person-specific features for the user and wherein at least one of the person-specific features in the first group always s selected and requested when identifying the user. However, Brookner teaches that a biometric feature can be the feature that is always selected in combination with the other data requested. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wizig to always choose at least one of the person-specific features based on the known principle that the use of biometrics for authentication is the strongest single-factor authentication and furthermore combining biometrics with another factor of authentication forms two-factor authentication which is also known to be better than single-factor authentication. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Brookner in col. 7, lines 32-46 and col. 26, lines 46-50.

As per claim 12:

Wizig, Ikebata et al., and Brookner substantially teach the method of claim 11. Furthermore, Brookner teaches wherein a plurality of the person-specific features are randomly selected and requested (col. 3, lines 55-57).

IV. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wizig, U.S. Patent No. 6,735,569, and further in view of Brookner, U.S. Patent No. 6,256,616.

As per claim 13:

Wizig substantially teaches a method for identifying a user, the method comprising the steps of providing a central server (col. 6, line 61 - col. 7, line 47 and fig. 1, element 200) with a database that includes plural different person-specific features of the user that are arranged in the database (col. 7, line 58 – col. 8, line 7 and fig. 2, element 1000) containing a second feature group that includes at least two of (a) the user name, (b) the date of birth, (c) a user number, and (d) a secret number (fig. 10); transmitting a request for the person-specific features from the central server to the user over a telecommunication network (col. 6, lines 15-24 and fig. 1, element 110); the user obtaining the requested person-specific feature at a user computer remote from the central server and transmitting the requested person-specific features to the central server over the telecommunication network (col. 10, line 32 – col. 11, line 31); and in the central server, comparing the person-specific features from the user to the features in the database to identify the user (col. 10, line 32 – col. 12, line 35).

Not explicitly disclosed is a central server with a database containing a first feature group comprising at least two of (a) a print from at least one finger, (b) the image of the iris of at least one eye, (c) a voice sample, (d) a sample signature, (e) an image of at least part of the user, and (f) the genetic fingerprint. However, Brookner teaches that identification can be based upon biometric data including a fingerprint, a voice sample, or retina eye scan used in combination with another form of identification. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wizig to use biometrics in

combination with another form of identification in order to have a stronger means of authentication based on the known principles that two-factor authentication is more secure than one-factor and that the use of biometrics as one of the two factors makes the combination of data required even more secure. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Brookner in col. 4, lines 1-41.

Also not explicitly disclosed is the central server randomly selecting one of the person-specific features from the first feature group and randomly selecting a further one of the person specific features from the first and second feature groups. However, Brookner teaches that the feature may be randomly selected. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wizig to randomly select additional information to request from the user during the process of authentication in order to diminish the possibility of an imposter to impersonate a legitimate user of the system. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Brookner in col. 3, lines 38-62.

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US Patent No. 6,772,336 has been cited because it is relevant due to the manner in which the invention has been claimed.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

Nadia Khoshnoodi
Examiner
Art Unit 2137
1/17/2006

NK